



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,909	08/28/2006	Masaya Yamamoto	2006_1366A	4375
52349 7590 01/27/2010 WENDEROTH, LIND & PONACK L.L.P. 1030 15th Street, N.W. Suite 400 East Washington, DC 20005-1503				
EXAMINER				
CHAI, LONGBIT				
ART UNIT		PAPER NUMBER		
2431				
MAIL DATE		DELIVERY MODE		
01/27/2010		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/590,909

Applicant(s)

YAMAMOTO ET AL.

Examiner

LONGBIT CHAI

Art Unit

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 December 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38, 41 and 42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-38, 41 and 42 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 August 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB06)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ ~~Notes of Informal Patent Application~~
- 6) ☐ Other: _____

DETAILED ACTION

- i. Currently pending claims are 1 – 38, 41 and 42.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, 35 and 37, Applicant asserts "a judgment unit operable to acquire, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used". Examiner respectfully disagrees with the following rationale:

- (a) Sako teaches "to improve security of medium bind key data MB_Key, it may not be recorded on the optical disc and medium bind key data MB_Key can be obtained through the network" (Sako: Para [0052] Line 9 – 11), i.e. for example, "alternatively, in a predetermined time period after medium bind key data has down loaded, it may be erased and then obtained from the WEB server" (Sako: Para [0061] Line 15 – 19: i.e. obtained from a source other than the recording medium at a certain time).
- (b) Examiner notes medium bind key data is qualified as contract information because Sako teaches "based on medium bind key data, the reproducing apparatus side or the server side can manage data with respect to DRM (Digital Rights Management) such as restriction about the number of copies of content data" (Sako: Para [0063] Line 5 – 10: i.e. whether the content is permitted to be used). Thereby, Applicant's arguments are respectfully traversed.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 41 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter where "A computer-readable recording medium" as recited in the claim alone has a lack of the required functional and structural interrelationship between the software and the computer storage medium that permits the functionality of the software to be realized / executed upon access by a processor. This ability is what underlies the ability to provide a practical application. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106 (IV.B).1(a). Such embodiments of the "manufacture" are not computer elements which define structural and functional interrelationships between the instructions and the rest of the computer that permit the functionality of the instructions to be realized / executed upon access by a processor. Examiner respectfully suggests an amendment of the claim language from "A computer-readable recording medium" to "*A computer-readable recording medium stores instructions executed upon access by a processor*" for clarity purpose. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 – 5, 7, 8, 10 – 28 and 30 – 38, 41 and 42 are rejected under 35 U.S.C. 102(b) as being anticipated by Sako et al. (U.S. Patent 2004/0030909) – which is more than one year prior to the date of application for patent in the United States filed on 3/1/2005 (371 U.S. filing date).

As per claim 1, 35 and 37, Sako teaches a content playback device for decrypting encrypted content recorded on a recording medium and playing back the decrypted content, comprising:

a read unit operable to read media information unique to the recording medium, from the recording medium (Sako: Figure 1 and Para [0031]);

a judgment unit operable to acquire, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used (Sako: Para [0028], Para [0052] Line 9 – 11 and Para [0063] Line 5 – 10:

(a) Sako teaches “to improve security of medium bind key data MB_Key, it may not be recorded on the optical disc and medium bind key data MB_Key can be obtained through the network” (Para [0052] Line 9 – 11), i.e. for example, “alternatively, in a predetermined time period after medium bind key data has down loaded, it may be erased and then obtained from the WEB server” (Sako: Para [0061] Line 15 – 19: i.e. obtained from a source other than the recording medium at a certain time), and (b) Examiner notes medium bind key data is qualified as contract information because Sako teaches “based on medium bind key data, the reproducing apparatus side or the server side can manage data with respect to DRM (Digital Rights Management) such as restriction about the number of copies of content data” (Para [0063] Line 5 – 10: i.e. whether the content is permitted to be used));

a generation unit operable to generate a content key based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used (Sako: Para [0029]);

a decryption unit operable to read the encrypted content from the recording medium, and decrypt the encrypted content using the generated content key (Sako: Para [0029]); and

a playback unit operable to play back the decrypted content (Sako: Figure 4A & 4B).

As per claim 41 – 42 (& claim 36 & 38), Sako teaches a recording medium storing:

first encrypted content protected by a first protection method and protection method information showing the first protection method, in correspondence with each other (Sako: Figure 1, Para [0028] and Para [0031]: (a) the content data or the medium bind key data which is encrypted is qualified as the first encrypted content and (b) the content key or a media key is qualified as one element of the corresponding first protection method); and

second encrypted content protected by a second protection method different from the first protection method and protection method information showing the second protection method, in correspondence with each other (Sako: Para [0028] Line 9 – 11: the data with DRM (i.e. license data) is encrypted – i.e. by a license key and thus the second protection method uses, e.g., a license key to encrypt the content key or a license key is used to decrypt the encrypted content key).

As per claim 2, Sako teaches the media information shows a media key which is assigned to the recording medium (Sako: Para [0031]), the contract information shows a license

key which is assigned to the contract (Sako: Para [0028] Line 9 – 11: the data with DRM (i.e. license data) is encrypted – i.e. by a license key), and the generation unit generates the content key based on the media key shown by the media information and the license key shown by the contract information (Sako: Para [0032]).

As per claim 3 and 21, Sako teaches the contract information includes a use condition of the encrypted content, and the judgment unit judges whether the encrypted content is permitted to be used, based on the use condition included in the contract information (Sako: Para [0028]).

As per claim 4 and 5, Sako teaches the recording medium stores generation method information in correspondence with the encrypted content, the generation method information showing whether the content key is to be generated using the license key, using the media key, or using both the license key and the media key, and the generation unit reads the generation method information from the recording medium, and generates the content key according to the read generation method information (Sako: Para [0032]: (a) the content key is required to be generated by both the license key and the media key, where the media key is MB_key and DEV_Key is part of the license key unique to application software installed to a personal computer) and (b) the hashing of both the license key and the media key, i.e. MB_key and DEV_Key generates the key locker key data that further generates the content key after the encrypted content key has been decrypted).

As per claim 7 and 8, Sako teaches the media information includes the media key which has been encrypted, and the generation unit decrypts the encrypted media key to obtain the media key (Sako: Figure 1 / Element 54 & 53: (a) a Medium Key Block key can be derived /

decrypted from a DEV_Key which is equivalent to a MKB_Key is encrypted by a device key DEV_Key (b) a device key DEV_Key is part of a read device information).

As per claim 10, Sako teaches the recording medium stores a content identifier for identifying the encrypted content, and the judgment unit reads the content identifier from the recording medium, and acquires the contract information corresponding to the read content identifier (Sako: Para [0011] and [0028]: identification data to identify the content and the associated license information stored with the content key and encrypted content).

As per claim 11, Sako teaches a storage unit operable to store the contract information beforehand; and a judging unit operable to read the contract information from the storage unit, and judge, based on the read contract information, whether the encrypted content is permitted to be used (Sako: Para [0028]).

As per claim 12, 25 and 32, Sako teaches the contract information is stored on another recording medium, in correspondence with the encrypted content, and the judgment unit acquires the contract information by reading the contract information from the other recording medium (Sako: Para [0063]).

As per claim 13, 26 and 33, Sako teaches a playback device being connected, via a network, to a server device for delivering the contract information, wherein the judgment unit acquires the contract information by receiving the contract information from the server device (Sako: Para [0063]).

As per claim 14, Sako teaches the generation unit is constituted by a removable module (Sako: Para [0005]: a medium/disc drive (or a recording apparatus) is qualified as a removable module).

As per claim 15, Sako teaches the generation unit and the judgment unit perform mutual authentication, the judgment unit outputs the contract information to the generation unit, if the judgment unit has succeeded in authenticating the generation unit, and the generation unit receives the contract information from the judgment unit and generates the content key, if the generation unit has succeeded in authenticating the judgment unit (Sako: Para [0005] / [0063] / [0047] and Para [0051] Line 7 – 9).

As per claim 16 and 17, Sako teaches the generation unit stores a first module identifier for identifying an invalid module, acquires an identifier for identifying the judgment unit, compares the acquired identifier with the first module identifier, and refuses to receive the contract information from the judgment unit if the acquired identifier matches the first module identifier (Sako: Para [0063] Line 7 – 18: a history of usage associated each recording / reproducing apparatus (i.e. a list of IDs) is tracked by a DRM server to control the license usage in order to identify a valid or invalid recording / reproducing apparatus / module that complies or violates the license agreement).

As per claim 18, Sako teaches for decrypting encrypted content recorded on a recording medium and playing back the decrypted content, at least first-type encrypted content that is protected by a first protection method and second-type encrypted content that is protected by a second protection method different from the first protection method being recorded on the

recording medium, and the encrypted content being any of the first-type encrypted content and the second-type encrypted content, the content playback device comprising: a reception unit operable to receive a designation of the encrypted content; an acquisition unit operable to acquire protection method information showing one of the first and second protection methods that is used for protecting the encrypted content (Sako: Figure 1 & and Para [0031] and Para [0028] Line 9 – 11: (a) the first protection method uses a media key, for example a medium-bind-key MB_Key, assigned to the recording medium and (b) the data with DRM (i.e. license data) is encrypted – i.e. by a license key and thus the second protection method uses, e.g., a license key); a generation unit operable to generate a content key corresponding to the acquired protection method information; a decryption unit operable to read the encrypted content from the recording medium, and decrypt the encrypted content using the generated content key; and a playback unit operable to play back the decrypted content (Sako: see claim 1 above).

As per claim 19, Sako teaches the first protection method uses a media key assigned to the recording medium, and the second protection method uses a license key assigned to a contract for use of the encrypted content (Sako: Figure 1 & and Para [0031] and Para [0028] Line 9 – 11: (a) the first protection method uses a media key, for example a medium-bind-key MB_Key, assigned to the recording medium and (b) the data with DRM (i.e. license data) is encrypted – i.e. by a license key and thus the second protection method uses, e.g., a license key), and the generation unit uses the media key to generate the content key if the protection method information shows the first protection method, and uses the license key to generate the content key if the protection method information shows the second protection method (Sako: Para [0032]: (a) the content key is required to be generated by both the license key and the media key, where the media key is MB_key and DEV_Key is part of the license key unique to

application software installed to a personal computer) and (b) the hashing of both the license key and the media key, i.e. MB_Key and DEV_Key generates the key locker key data that further generates the content key after the encrypted content key has been decrypted).

As per claim 20, Sako teaches the recording medium stores the protection method information in correspondence with the encrypted content, and the acquisition unit acquires the protection method information by reading the protection method information from the recording medium (Sako: Para [0061] Line 12 – 18: the protecting method is depending upon whether the medium key has yet been erased that is based on the management information such as the time period and the number of copies of license usage).

As per claim 22, Sako teaches the protection method information includes a content identifier for identifying the encrypted content and key type information showing a type of the content key, and the generation unit generates the content key which corresponds to the encrypted content identified by the content identifier and is of the type shown by the key type information (Sako: Para [0061] / [0064] / [0065]: the type of content keys is defined by whether the medium key is still stored at the recording medium or the medium key need to be read from the WEB server).

As per claim 23, Sako teaches key type information showing a type of the content key accompanies the encrypted content on the recording medium, the acquisition unit reads the key type information from the recording medium, and the generation unit generates the content key of the type shown by the read key type information (Sako: Para [0061] / [0064] / [0065] and Para [0028]: the type of content keys is defined by whether the medium key is still stored at the

recording medium or the medium key need to be read from the WEB server and this content key type information is depending on and related to the management information stored at the recording medium together with the encrypted content).

As per claim 24, Sako teaches the key type information is multiplexed with the encrypted content on the recording medium, and the acquisition unit separates the key type information from the encrypted content (Sako: Para [0061] / [0064] / [0065] and Para [0028]: the content key type information is depending on and related to the management information stored at the recording medium together with the encrypted content).

As per claim 27, Sako teaches the recording medium stores media information showing the media key, and the generation unit uses the media key shown by the media information (Sako: Figure 1 and Para [0031]).

As per claim 28, Sako teaches the media information includes the media key which has been encrypted using device information unique to the content playback device, and the generation unit reads the device information held in the content playback device, and decrypts the encrypted media key using the read device information to obtain the media key (Sako: Figure 1 / Element 54 & 53: (a) a Medium Key Block key can be derived / decrypted from a DEV_Key which is equivalent to a MKB_Key is encrypted by a device key DEV_Key and (b) a device key DEV_Key is part of a read device information).

As per claim 30, Sako teaches the recording medium stores a content identifier for identifying the encrypted content, and the generation unit reads the content identifier from the

recording medium, and uses the license key corresponding to the content identifier (Sako: Para [0018] and Para [0028] Line 9 – 11: (a) content data identifier and (b) the data with DRM (i.e. license data) is encrypted – i.e. by a license key and thus the second protection method uses, e.g., a license key).

As per claim 31, Sako teaches storing contract information including the license key, beforehand; and a generating unit operable to read the contract information from the storage unit and generate the content key using the license key included in the read contract information, if the protection method information shows the second protection method (Sako: Para [0028] Line 9 – 11: the data with DRM (i.e. license data) is encrypted – i.e. by a license key and thus the second protection method uses, e.g., a license key which is also used to decrypt the encrypted content key).

As per claim 34, Sako teaches the recording medium stores content information unique to the encrypted content, in correspondence with the encrypted content, and the generation unit generates the content key using the media key and the content information, if the protection method information shows the first protection method Sako: Para [0032]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 6, 9 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sako et al. (U.S. Patent 2004/0030909), in view of Peinado et al. (U.S. Patent 6,772,340).

As per claim 6, Sako does not disclose expressly the contract information includes the license key, as the content key.

Peinado teaches the contract information includes the license key, as the content key (Peinado: Column 3 Line 13 – 23 / Line 53 – 54: the contract information includes the content key (i.e. decryption key KD) which is also the license key that encrypts the license term).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Peinado within the system of Sako because (a) Sako teaches a mechanism how to manage the DRM (Digital Rights Management) in a recording medium (Sako: Para [0028]) and (b) Peinado teaches an effective digital rights management system where the contract information includes the content key (i.e. decryption key KD) which is also the license key that can encrypt the license term (Peinado: Column 3 Line 13 – 23 / Line 53 – 54).

Accordingly, Sako in view of Peinado teaches:

the content key, which has been encrypted using the media key, and if the generation method information shows that the content key is to be generated using both the license key and the media key, the generation unit decrypts the encrypted license key using the media key to generate the content key (Sako: Para [0029]) & (Peinado: Column 3 Line 13 – 23 / Line 53 – 54: the contract information includes the content key (i.e. decryption key KD) which is also the license key that encrypts the license term).

As per claim 9 and 29, Sako does not disclose expressly the judgment unit reads the contract identifier from the recording medium, and acquires the contract information identified by the read contract identifier.

Peinado teaches the judgment unit reads the contract identifier from the recording medium, and acquires the contract information identified by the read contract identifier (Peinado: Column 3 Line 22 – 23: a license signature is qualified as the contract identifier).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Peinado within the system of Sako because (a) Sako teaches a mechanism how to manage the DRM (Digital Rights Management) in a recording medium (Sako: Para [0028]) and (b) Peinado teaches an effective digital rights management system where a license signature can be served as the contract identifier the contract information includes the content key (i.e. decryption key KD) which is also the license key that can encrypt the license term (Peinado: Column 3 Line 13 – 23 / Line 53 – 54).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Examiner, Art Unit 2431
1/13/2010